UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF OKLAHOMA

GUADALUPE GRANADO; MANUEL VEGA; and DONALD JOHNSTON, individually and on behalf of all similarly situated persons, Plaintiffs, v. SANDRIDGE ENERGY, INC., Defendant.	Case No.: 5:22-cv-00516 **JURY TRIAL DEMANDED**

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs Guadalupe Granado, Donald Johnston, and Manuel Vega, individually and on behalf of all others similarly situated (collectively "Plaintiffs" individually "Mr. Granado", "Mr. Johnston", or "Mr. Vega"), upon personal knowledge of facts pertaining to themselves and upon information and belief as to all other matters, and by and through undersigned counsel, hereby bring this First Amended Class Action Complaint against Defendant, SandRidge Energy, Inc. ("SandRidge" or "Defendant"), and allege as follows:

INTRODUCTION

1. Plaintiffs bring this class action against Defendant on behalf of themselves and all others similarly situated for Defendant's failure to properly secure and safeguard Plaintiffs' and Class members' personally identifiable information stored within Defendant's information network, including, without limitation, first and last names in combination with their Social Security numbers (this type of information, *inter alia*, being hereafter referred to as "personally identifiable information" or "PII").[1]

[1] Personally identifiable information generally incorporates information that can be used

2. With this action, Plaintiffs seek to hold Defendant responsible for the harms it caused Plaintiffs and the over twelve thousand (12,000) other similarly situated Class members in the massive and preventable ransomware attack that took place beginning on or around October 25, 2021, in which cybercriminals infiltrated Defendant's inadequately protected network servers where highly sensitive personal information was being kept unprotected (the "Data Breach" or "Breach").

3. Defendant claims that on October 25, 2021, it experienced a "network disruption" in which "limited information maintained on our network was accessed by an unauthorized actor." *See* **Exhibit** 1, Notice of Data Breach (the "Notice Letter").

4. This PII was compromised due to Defendant's negligent, grossly negligent, and/or reckless acts and omissions and the failure to protect PII of Plaintiff and Class members.

5. Due to Defendant's negligence, gross negligence, and/or recklessness and data security failures, cybercriminals obtained and now possess everything they need to commit personal identity theft and wreak havoc on the financial and personal lives of thousands of individuals for decades to come.

6. Defendant flagrantly disregarded Plaintiffs' and Class members' privacy and property rights by intentionally, willfully, and recklessly failing to take the necessary precautions required to safeguard and protect Plaintiffs' and other Class members' PII from unauthorized disclosure. Plaintiffs' and Class members' PII was improperly handled,

---

to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

inadequately protected, readily able to be copied by thieves, and not kept in accordance with basic security protocols. Defendant's obtaining of the information and sharing of the same also represents a flagrant disregard of Plaintiffs' and Class members' rights, both as to privacy and property.

7. The exposed PII of Plaintiffs and Class members can be sold on the dark web, used to commit further cyberattacks, or used for identity theft and fraud. Once released from its secured location, PII is forever compromised and victims must guard against its misuse for the remainder of their lives. Given Defendant's misconduct in allowing hackers to access such information in this instance, Plaintiffs and Class members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

8. As a result of the Data Breach, Plaintiffs and Class members have already suffered damages. For example, now that their PII has been obtained by cybercriminals, Plaintiffs and Class members are at imminent and impending risk of identity theft and must constantly monitor their accounts and transactions for attempts at fraud and identity theft. This risk will continue for the rest of their lives. Additionally, Plaintiffs and Class members have already lost time and money responding to and mitigating the impact of the Data Breach, and those efforts are continuous and ongoing.

9. Plaintiffs and the Class have also suffered and are entitled to damages for the lost benefit of the bargain with Defendant. Plaintiffs and members of the Class were required to provide their PII to Defendant as a condition of their employment and implicit in this exchange was that Defendant would keep Plaintiffs' and Class members' PII safe and that it would destroy the PII of employees and former employees that was no longer necessary to maintain. Defendant's failure to implement adequate security measures to protect the PII of

Plaintiffs and Class members constituted a denial of Plaintiffs' and Class members' expected benefit of the contract between the parties. In that respect, Plaintiffs and Class members have not received the benefit of the bargain and have suffered an ascertainable loss.

10. Additionally, because of Defendant's conduct, Plaintiffs and Class members have been harmed in that Defendant breached its common law fiduciary duty of confidentiality owed to Plaintiffs and Class members.

11. Defendant acquired, collected, and stored Plaintiffs' and Class members' PII as a condition of Plaintiffs' and Class members' employment.

12. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class members' PII, Defendant assumed legal and equitable duties to those individuals. These duties arise from state and federal statutes and regulations as well as common law principles.

13. Defendant disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs' and Class members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. Defendant also improperly retained PII for longer than was necessary and allowed it to be accessed in the Data Breach. As a result, the PII of Plaintiffs and Class members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit from the PII stolen in this Data Breach.

14. Because Defendant has experienced a Data Breach there is a strong likelihood that Defendant will again be targeted by cyber criminals for the PII of Plaintiffs and Class

members. This PII remains in the custody of Defendant and Plaintiffs and Class members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

15. Defendant violated its duty to Plaintiffs and Class members through its failure to protect against a foreseeable cyber-attack.

THE PARTIES

16. Defendant SandRidge is a foreign for-profit business corporation incorporated in the State of Delaware. It is headquartered in Oklahoma County.

17. Defendant is "an independent oil and gas company engaged in the development and acquisition of oil and gas properties. Its primary areas of operation are the Mid-Continent in Oklahoma and Kansas."[2]

18. Defendant was founded in 2006 and "employs approximately 100 people and generates annual revenue of $144 million."[3]

19. Plaintiff Granado is a resident of Pecos County, Texas and is a former employee of SandRidge who worked for Defendant until 2007.

20. Plaintiff Vega is a resident of Garfield County, Oklahoma and is a former employee of SandRidge who worked for Defendant until 2014.

21. Plaintiff Johnston is a resident of Oklahoma County, Oklahoma and is a former employee of SandRidge who worked for Defendant until 2017.

22. Plaintiffs and the proposed Class members are current or former employees of

[2] *See* https://sandridgeenergy.com/ (last accessed May 20, 2022).
[3] *See* https://www.jdsupra.com/legalnews/sandridge-energy-llc-files-notice-of-3563322/#:~:text=SandRidge%20Energy%2C%20LLC%2C%20based%20in,of%20certain%20individuals%20being%20compromised. (last accessed May 23, 2022).

Defendant. As part of its business operation, Defendant collects and maintains the PII of its employees and, apparently former employees.[4]

23. Plaintiffs entered into an implied contract with Defendant for the adequate protection of their PII.

24. When Plaintiffs entered into employment relationships with Defendant, they reasonably believed that Defendant would keep their PII secure and would delete it following the termination of the employment relationship. Had Defendant disclosed to them that their PII would not be kept secure and would be easily accessible to criminal hackers and third parties, they would have demanded Defendant take additional precautions relating to their PII, would have demanded a higher salary, or would not have worked for Defendant at all.

JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than one hundred putative class members, and minimal diversity exists because many putative class members are citizens of a different state than Defendant.

26. The Western District of Oklahoma has personal jurisdiction over Defendant because Defendant is incorporated and has its principal place of business in this District; conducts substantial business in this District through its headquarters, offices, and affiliates; engaged in the conduct at issue here in this District; and otherwise has substantial contacts with this District and purposely availed itself to the Courts in this District.

[4] Any reference to "employee" herein shall include current employees, former employees, or job applicants.

27. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant's principal place of business is in this District.

FACTUAL ALLEGATIONS

A. Defendant's inadequate data security exposed its current and former employees' sensitive PII

28. Beginning on or around October 25, 2021, an unknown criminal actor targeted and gained access to Defendant's computer network where highly sensitive employee PII was contained unencrypted.

29. Plaintiffs who had most recently worked for Defendant in 2014, received letters from Defendant dated March 31, 2022, in which Defendant provided notice of the Breach (the "Notice Letter").

30. The Notice Letters were sent to Plaintiffs and the Class more than five months after the Data Breach occurred and included the following:

> **What Happened:**
>
> On October 25, 2021, we experienced a network disruption that impacted certain systems. Upon discovery, we took immediate action to address and investigate the incident, which included engaging third-party specialists to assist with determining the nature and scope of the incident. A thorough investigation determined that limited information maintained on our network was accessed by an unauthorized actor. We then began a thorough and time intensive review of the contents of the data to determine the type of information contained within our files and to whom that information related. On February 28, 2022, this review was completed and we immediately worked to obtain up-to-date address information in order to provide you with this notice. On March 17, 2022, this process was completed.
>
> **What Information Was Involved:**

> The types of information contained within the affected data included your first and last name, in combination with the following data element(s): Social Security number.
>
> **What We Are Doing:**
>
> We have taken the steps necessary to address this incident and are committed to fully protecting all of the information that you have entrusted to us. Upon learning of this incident, we immediately took steps to secure our systems and undertook a thorough investigation. We have also implemented additional technical safeguards to further enhance the security of information in our possession and to prevent similar incidents from happening in the future. Additionally, we are offering you complimentary credit monitoring and identity protection services.

31. After receiving the Notice Letters, it is reasonable for recipients, including Plaintiffs and Class members, to believe that the risk of future harm (including identity theft) is substantial and imminent, and that it its necessary for them to take steps to mitigate that substantial risk of impending and future harm. Indeed, Defendant admonishes victims of the Data Breach to "remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors." Defendant also offered complimentary access to Equifax Credit Watch™ Gold for twelve (12) months, an offer it need not have provided absent any threat to Plaintiffs and the Class. *See* **Exhibit 1**.

32. Upon information and belief, the unauthorized third-party cybercriminals intentionally targeted and gained access to the PII with the intent of engaging in misuse of the PII, including marketing and selling Plaintiffs' and Class members' PII to fraudsters as that is the *modus operandi* of data thieves.

33. Despite the severity of the Data Breach, Defendant has done very little to protect Plaintiffs and the Class or to compensate them for their lost time, diminished value of their PII, or expenses they incur as a result. For example, in the Notice Letter, Defendant only provides twelve (12) months of identity theft and credit monitoring protection. This

complimentary service is a token gesture that does little if anything to remedy the harm Defendant's misconduct caused. This does not and will not fully protect the employees and former employees from cybercriminals and is largely ineffective against protecting data after it has been stolen. Cybercriminals are fully aware of the well-publicized preventative measures taken by entities after data breaches such as that which happened here and will, therefore, oftentimes hold onto the stolen data and not use it until after the complimentary service is no longer active, and long after victim concerns and preventative steps have diminished.

34. In effect, Defendant is shirking its responsibility for the harm and increased risk of harm it has caused Plaintiffs and members of the Class, including the distress and financial burden the Data Breach has placed upon the shoulders of the Data Breach victims.

35. The Notice Letter fails to provide the consolation Plaintiffs and Class members seek and certainly falls far short of eliminating the substantial risk of fraud and identity theft Plaintiffs and the Class now face.

36. To make matters worse, Defendant's attackers intentionally targeted and gained access to Plaintiffs' and Class members' PII. While many ransomware attacks merely involve the attacker gaining control of the computer or network without access to the victims' information, the ransomware attack on Defendant's systems gave the attackers access to Plaintiffs' and Class members' PII.

37. Plaintiffs' and Class members' information is likely for sale on the dark web as each has discovered misuse of their PII since the Data Breach. Their PII could also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and/or Class members. Either way, unauthorized individuals can easily access and misuse the PII of Plaintiffs and Class members.

B. The Cyber-attackers acted with actual malice

38. The cyber-attackers here acted with actual malice, with a criminal motive, Plaintiffs' and Class members' data has been exposed as the result of a targeted attempt to obtain that data. Defendant's investigation into the attack confirmed its network was intentionally breached on October 25, 2021.

39. According to information Defendant provided to the Office of the Attorney General for the State of Maine, the Data Breach was conducted via ransomware.[5]

40. The parts of the network accessed by the attackers contained employees' unsecured PII. The Notice Letter states: "[A] thorough investigation determined that limited information maintained on our network was accessed by an unauthorized actor." *See* **Exhibit 1**.

41. Ransomware attacks are typically the last phase of a multi-pronged cyberattack that is targeted at confidential data. The prime motivation of ransomware is the theft of confidential data like the Social Security numbers stolen here. A recent analysis shows that data exfiltration occurs in 70% of all ransomware attacks.[6] Ransomware attacks are often used to distract security teams because "it provides the perfect cover to distract attention so they can take aim at their real target: exfiltrating IP, research, and other valuable data."[7]

---

[5] *See* *https://apps.web.maine.gov/online/aeviewer/ME/40/8a95d0d5-8955-4eec-a77b-c60caa1c3975.shtml*. (Last accessed May 23, 2022).

[7] Jessica Davis, *70% Ransomware Attacks Cause Data Exfiltration; Phishing Top Entry Point*, HealthITSecurity (Feb. 3, 2021), https://healthitsecurity.com/news/70-ransomware-attacks-cause-data-exfiltration-phishing-top-entry-point.

[7] *Ransomware provides the perfect cover*, available at https://www.helpnetsecurity.com/2021/01/21/ransomware-cover/

42. Ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[8] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."[9] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[10] And even where companies pay for the return of data, attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[11]

C. Plaintiffs have suffered actual misuse as a result of this Data Breach

43. Plaintiff Granado has suffered actual misuse of his PII as a result of this Data Breach. As described more fully below, Plaintiff recently discovered his credit score has dropped dramatically and believes it may be as a result of the Data Breach.

44. Plaintiff Vega has suffered actual misuse of his PII as a result of this Data Breach. As described more fully below, Plaintiff Vega experienced a fraud attempt on his debit card in May of 2022, shortly after he received the Notice Letter.

45. Plaintiff Donald Johnston has suffered actual misuse of his PII as a result of this Data Breach. As described more fully below, Plaintiff Johnston has started experiencing an influx of spam emails that he did not sign-up for shortly after he received the Notice Letter.

---

[8] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends

[9] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/

[10] *Id.*

[11] *Id.*

D. The type of data compromised here can be used for fraud and identity theft

46. The type of data that was accessed and compromised here (including full names and Social Security numbers) can easily be used to perpetrate fraud and identity theft. Social Security numbers are widely regarded as the most sensitive information hackers can access due to their durability.

47. Social Security numbers are the "gold standard" for identity theft.

48. Experience and common sense teach that Plaintiffs face a substantial risk of identity theft given that their Social Security numbers and name were intentionally targeted and accessed by a criminal intruder.

49. When a Social Security number is stolen it can forever be wielded to identify the victim and target him/her in fraudulent schemes and identity theft attacks and it appears that for Plaintiffs it already has been as a result of the Data Breach.

E. The PII exposed by Defendant as a result of its inadequate data security is highly valuable on the black market

50. The information targeted in the attack and exposed by Defendant is a virtual goldmine for phishers, hackers, identity thieves and cybercriminals.

51. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

52. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, that stolen information often ends up on the dark web because the

malicious actors buy and sell that information for profit.[12]

53. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[13]

54. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200[14]. Criminals can also purchase access to entire company data breaches from $900 to $4,500[15].

55. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are

---

[12] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last accessed July 28, 2021).

[13] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:* https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last accessed July 28, 2021).

[14] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 28, 2021).

[15] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 28, 2021).

difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems[16].

56. What is more, is it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

57. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

58. Because of this, the information compromised in the Data Breach here is significantly more harmful to lose than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts.

---

[16] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 28, 2021).

[17] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited July 28, 2021).

The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

59. The PII compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[18]

60. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends, and colleagues of the original victim.

61. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

62. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiffs and Class members that their PII had been stolen. It took Defendant more than five months to notify Plaintiffs of the compromise.

63. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

[18] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 28, 2021).

64. Data breaches facilitate identity theft as hackers intentionally target and obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

F. Defendant failed to comply with Federal Trade Commission requirements

65. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[19]

66. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[20] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[21]

67. Additionally, the FTC recommends that companies limit access to sensitive

---

[19] *See* Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 28, 2021).

[20] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 28, 2021).

[21] *Id.*

data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[22]

68. Highlighting the importance of protecting against phishing and other types of data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[23]

69. By negligently securing Plaintiffs' and Class members' PII and allowing an unknown third-party cyber-attacker to access Defendant's unencrypted, unprotected PII, Defendant failed to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data. Defendant's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

G. Defendant collected, stored, and maintained Plaintiffs' and Class Members' PII

70. Defendant acquired, collected, and stored Plaintiffs' and Class members' PII.

71. At all relevant times, Defendant knew or should have known that its employees were required to store and/or share sensitive data with it, including highly confidential PII.

---

[22] Federal Trade Commission, *Start With Security*, *supra footnote 17*.

[23] Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited July 28, 2021).

72. Plaintiffs and members of the Class were required to provide their PII to Defendant as a condition of their employment. Implicit in this exchange was that Defendant would keep Plaintiffs' and Class members' PII safe and would delete it once it was no longer necessary to maintain the PII. Plaintiffs and Class members would not have provided their PII, would have demanded higher pay, or would not have worked for Defendant at all had they known that Defendant would not safeguard their PII. Defendant's failure to implement adequate security measures to protect the PII of Plaintiffs and Class members constituted a denial of Plaintiffs' and Class members' expected benefit of the contract between the parties.

73. By obtaining, collecting, and storing Plaintiffs' and Class members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class members' PII from unauthorized disclosure.

74. Plaintiffs and Class members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

75. Defendant could have prevented this Data Breach by properly securing and encrypting Plaintiffs' and Class members' PII.

76. Defendant's negligence in safeguarding Plaintiffs' and Class members' PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

77. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being

compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of the Class.

78. Defendant owed a duty to Plaintiffs and the Class to design, maintain, and test its computer systems and networks to ensure that the PII in its possession was adequately secured and protected.

79. Defendant owed a duty to Plaintiffs and the Class to create and implement reasonable data security practices and procedures to protect the PII in its possession.

80. Defendant owed a duty to Plaintiffs and the Class to implement processes that would detect a breach on its data security systems in a timely manner.

81. Defendant owed a duty to Plaintiffs and the Class to act upon data security warnings and alerts in a timely fashion.

82. Defendant owed a duty to Plaintiffs and the Class to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust PII with Defendant.

83. Defendant owed a duty of care to Plaintiffs and the Class because they were foreseeable and probable victims of any inadequate data security practices.

84. Defendant owed a duty to Plaintiffs and the Class to encrypt Plaintiffs' and Class members' PII and monitor user behavior and activity in order to identity possible threats.

85. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, the criminal(s) and/or their customers now have Plaintiffs' and the other Class members' compromised PII.

86. There is a robust international market for the purloined PII. Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the other Class members at an imminent, immediate, and continuing increased risk of identity theft, identity fraud[24] and medical fraud.

87. Defendant flagrantly disregarded and/or violated Plaintiffs' and Class members' privacy and property rights, and harmed them in the process, by not obtaining Plaintiffs' and Class members' prior written consent to disclose their PII to any other person as required by laws, regulations, industry standards and/or internal company standards.

88. Defendant flagrantly disregarded and/or violated Plaintiffs' and Class members' privacy and property rights, and harmed them in the process, by failing to safeguard and protect and, in fact, wrongfully disseminating Plaintiffs' and other Class members' PII to unauthorized persons.

H. The value of PII

89. The data accessed in such an attack represents a major score for cybercriminals. This information is of great value to them, and the data stolen in the Data Breach will be used in a variety of sordid ways for criminals to exploit Plaintiffs and the Class members and to profit off their misfortune.

[24]According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia*, credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services).

90. Indeed, it is well known and the subject of many media reports that PII is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches of corporate entities, Defendant maintained an insufficient and inadequate system to protect the PII of Plaintiffs and Class members.

91. PII is a valuable commodity for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on a number of underground Internet websites.

92. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[25] For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[26] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class members.

93. Indeed, it is well known and the subject of many media reports that PII is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches of corporate entities, Defendant maintained an insufficient and inadequate system to protect the PII of Plaintiffs and Class members.

---

[25] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[26] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/. (last accessed July 28, 2021).

94. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.

95. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Plaintiff and Class members for the rest of their lives. They will need to remain constantly vigilant for identity theft.

96. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

97. Identity thieves can use personal information, such as that of Plaintiffs and Class members which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

98. The ramifications of Defendant's failure to keep secure Plaintiffs' and Class members' PII are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

99. The PII of Plaintiffs and Class members was targeted and taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years for some Class members.

100. In this context, at all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Plaintiffs' and Class members' PII, including Social Security numbers and/or dates of birth, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class members as a result of a breach.

101. As a result of the Data Breach, the PII of Plaintiffs and Class members has been exposed to criminals for misuse. The injuries suffered by Plaintiffs and Class members, or likely to be suffered thereby as a direct result of Defendant's Data Breach, include:

a. unauthorized use of their PII;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PII;

e. Improper disclosure of their PII;

f. loss of privacy, and embarrassment;

g. trespass and damage their personal property, including PII;

h. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach;

i. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet black market; and

j. damages to and diminution in value of their PII entrusted to Defendant for the sole purpose of employment by Defendant; and the loss of Plaintiffs' and Class members' privacy.

102. The injuries to the Plaintiffs and Class members were directly and proximately cause by Defendant's failure to implement or maintain adequate data security measures for this PII.

103. The Data Breach was the inevitable result of Defendant's inadequate approach to data security and the protection of the PII that it collected during the course of business and, as such, Defendant could have prevented this Data Breach. It had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

104. Had Defendant remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the Data Breach and, ultimately, the theft of its employees' PII.

105. Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Class members are incurring and will continue to incur such damages in addition to any actual fraudulent usage of their PII.

106. The injuries to Plaintiffs and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class members.

107. This was a financially motivated and targeted Data Breach, as apparent from the ransom money sought by the cybercriminals, who will continue to seek to profit off of the sale of Plaintiffs' and the Class members' PII on the dark web. The PII exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein.

108. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[27]

109. Data breaches are preventable.[28] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of

[27] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info. (last accessed July 28, 2021).

[28] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

appropriate security solutions."[29] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[30]

110. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[31]

111. Defendant required Plaintiffs and Class members to surrender their PII – including but not limited to their names and Social Security numbers – and was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of such PII.

112. Many failures laid the groundwork for the success ("success" from the cyber-attackers' viewpoint) of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security protections, procedures, and protocols necessary to safeguard Plaintiff's and Class members' PII. Yet it did not do so.

113. Defendant knew of the importance of safeguarding Plaintiffs' and Class members' PII and of the foreseeable consequences that would occur if Plaintiffs' and Class members' PII was stolen, including the significant costs that would be placed on Plaintiffs and Class members as a result of a breach of this magnitude.

114. Defendant is a sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiffs, Class

---

29 *Id.* at 17.
30 *Id.* at 28.
31 *Id.*

members, and all its employees. Its failure to do so is, therefore, intentional, willful, reckless and/or grossly negligent.

115. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiffs' and Class members' PII from those risks left that information in a dangerous condition.

116. Defendant disregarded the rights of Plaintiffs and Class members by, inter alia, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class members prompt and accurate notice of the Data Breach.

117. The actual and adverse effects to Plaintiffs and Class members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendant's wrongful actions and/or inaction, *infra*, and the resulting Data Breach require Plaintiff and Class members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost.

Plaintiff and other Class members have suffered, and will continue to suffer, such damages for the foreseeable future.

I. Plaintiff Granado's experience

110. Plaintiff Granado is a former employee of Defendant. He worked as a roughneck for Defendant from approximately 2007-2009. Plaintiff Granado agreed to entrust his PII to Defendant as a condition of receiving employment and elective benefits. In exchange Defendant agreed, not only to accept his PII, but also to safeguard it and delete it following the termination of the employment relationship. Neither Plaintiff Granado nor Defendant reasonably expected that Plaintiff Granado was providing his PII to Defendant forever.

111. In or around April 2022, Plaintiff received a notice letter from Defendant informing him that his PII "was accessed by an unauthorized actor" in the Data Breach and that he must "remain vigilant against incidents of identity theft and fraud."

112. Unfortunately for Plaintiff Granado, this warning came too late. Plaintiff Granado had been in the process of applying for a home loan. Between the date of the Data Breach and prior to his receiving notice of the Data Breach, Plaintiff Granado learned that his credit score had dropped dramatically but was unsure why. Then, he learned of the Data Breach upon receiving notice from Defendant more than five months after the Data Breach occurred. Thus, Plaintiff Granado logically believes that his credit has been negatively affected as a direct and proximate result of the Data Breach.

113. Plaintiff Granado suffered economic harm because his low credit score delayed his approval for a home loan due to derogatory marks within his credit report that he believes result from the misuse of his PII.

114. As a direct and traceable result of the Data Breach, Plaintiff Granado has been

forced to spend time dealing with and responding to the direct consequences of the Data Breach, which includes researching the Data Breach and reviewing his credit report. This is time that he spent at Defendant's direction and that has been lost forever and cannot be recaptured.

115. Plaintiff Granado has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. He deletes any and all electronic documents containing his PII and destroys any documents that may contain any of his PII, or that may contain any information that could otherwise be used to compromise his PII.

116. Plaintiff Granado has suffered actual, concrete injury in the form of damages to, and diminution in, the value of his PII – a form of intangible property that Plaintiff Granado entrusted to Defendant for the purpose of his employment. His PII was compromised in, and has been diminished as a result of, the Data Breach. The harm to his PII resulting from the Data Breach is evidenced by his diminished credit score which prevented him from securing a timely and favorable loan.

117. Plaintiff Granado has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress, anxiety, and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

118. Plaintiff Granado has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII resulting from the compromise of his PII, especially his Social Security number, in combination with his full name, which is now in the hands of cybercriminals and other unauthorized third parties.

119. Knowing that thieves intentionally targeted and stole his PII, including his

Social Security number, and knowing that, based on the harm to his credit score, his PII has likely been sold on the dark web has caused Plaintiff great anxiety.

120. Plaintiff Granado has a continuing interest in ensuring that his PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

121. As a direct and traceable result of the Data Breach, Plaintiff Granado will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come and will have to pay an identity monitoring company for the rest of his life to protect his exposed PII.

J. Plaintiff Vega's Experience

122. Plaintiff Vega is a former employee of Defendant and worked for Defendant until November of 2014. Plaintiff Vega agreed to entrust his PII to Defendant as a condition of receiving employment and elective benefits. In exchange Defendant agreed, not only to accept his PII, but also to safeguard it and delete it following the termination of the employment relationship. Neither Plaintiff Vega nor Defendant reasonably expected that Plaintiff Vega was providing his PII to Defendant forever.

123. In or around April 2022, Plaintiff Vega received a notice letter from Defendant informing him that his PII "was accessed by an unauthorized actor" in the Data Breach and that he must "remain vigilant against incidents of identity theft and fraud."

124. Shortly after Plaintiff Vega received the Notice Letter, in May of 2022, he received a warning from his bank that his debit card was being used to make fraudulent transactions. Plaintiff Vega had never been warned of or experienced a fraudulent transaction on any of his accounts prior to this and does not share his PII or financial information with

others. Accordingly, Plaintiff Vega logically believes the fraudulent use of his debit card was a direct and proximate result of the Data Breach.

125. Plaintiff Vega suffered harm because his PII was intentionally targeted in the Data Breach and subsequently misused to his detriment.

126. As a direct and traceable result of the Data Breach, Plaintiff Vega has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which includes researching the Data Breach, reviewing his credit report, and changing his debit card account. This is time that he spent at Defendant's direction and that has been lost forever and cannot be recaptured.

127. Plaintiff Vega has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. He deletes any and all electronic documents containing his PII and destroys any documents that may contain any of his PII, or that may contain any information that could otherwise be used to compromise his PII.

128. Plaintiff Vega has suffered actual, concrete injury in the form of damages to, and diminution in, the value of his PII – a form of intangible property that Plaintiff Vega entrusted to Defendant for the purpose of his employment. His PII was compromised in, and has been diminished as a result of, the Data Breach. The harm to his PII resulting from the Data Breach is evidenced by the fact that identity thieves can access his financial accounts using his Social Security number and name.

129. Plaintiff Vega has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress, anxiety, and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

130. Plaintiff Vega has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII resulting from the compromise of his PII, especially his Social Security number, in combination with his full name, which is now in the hands of cybercriminals and other unauthorized third parties.

131. Knowing that thieves intentionally targeted and stole his PII, including his Social Security number, and knowing that, based on the misuse of his debit card, his PII has likely been sold on the dark web has caused Plaintiff Vega great anxiety.

132. Plaintiff Vega has a continuing interest in ensuring that his PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

133. As a direct and traceable result of the Data Breach, Plaintiff Vega suffered the misuse of his PII and will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come and will have to pay an identity monitoring company for the rest of his life to protect his exposed PII.

K. Plaintiff Johnston's Experience

134. Plaintiff Johnston is a former employee of Defendant and worked for Defendant until 2017. Plaintiff Johnston agreed to entrust his PII to Defendant as a condition of receiving employment and elective benefits. In exchange Defendant agreed, not only to accept his PII, but also to safeguard it and delete it following the termination of the employment relationship. Neither Plaintiff Johnston nor Defendant reasonably expected that Plaintiff Johnston was providing his PII to Defendant forever.

135. In or around late March 2022 or early April 2022, Plaintiff Johnston received a notice letter from Defendant informing him that his PII "was accessed by an unauthorized

actor" in the Data Breach and that he must "remain vigilant against incidents of identity theft and fraud."

136. Shortly after Plaintiff Johnston received the Notice Letter, Plaintiff Johnston started receiving a large volume of spam emails to his email address. The emails he received included insurance solicitations, food advertisements, and solicitations to sell his car and house. Plaintiff Johnston did not sign up to receive these emails, but he is still currently receiving them. Accordingly, Plaintiff Johnston logically believes the spam emails he is receiving are a direct and proximate result of the Data Breach.

137. Plaintiff Johnston suffered harm because his PII was intentionally targeted in the Data Breach and subsequently misused to his detriment.

138. As a direct and traceable result of the Data Breach, Plaintiff Johnston has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which includes researching the Data Breach, reviewing his credit report, and sifting through numerous spam emails. This is time that he spent at Defendant's direction and that has been lost forever and cannot be recaptured.

139. Plaintiff Johnston has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. He deletes any and all electronic documents containing his PII and destroys any documents that may contain any of his PII, or that may contain any information that could otherwise be used to compromise his PII.

140. Plaintiff Johnston has suffered actual, concrete injury in the form of damages to, and diminution in, the value of his PII – a form of intangible property that Plaintiff Johnston entrusted to Defendant for the purpose of his employment. His PII was compromised in, and has been diminished as a result of, the Data Breach. The harm to his PII resulting from the

Data Breach is evidenced by the fact that his email address has been distributed others without his consent.

141. Plaintiff Johnston has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress, anxiety, and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

142. Plaintiff Johnston has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII resulting from the compromise of his PII, in combination with his full name, which is now in the hands of cybercriminals and other unauthorized third parties.

143. Knowing that thieves intentionally targeted and stole his PII, including his Social Security number, and knowing that, based on the increased volume and frequency of spam emails he has received since the Data Breach, his PII has likely been sold on the dark web, Plaintiff Johnston has experienced great anxiety.

144. Plaintiff Johnston has a continuing interest in ensuring that his PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

145. As a direct and traceable result of the Data Breach, Plaintiff Johnston suffered the misuse of his PII and will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come and will have to pay an identity monitoring company for the rest of his life to protect his exposed PII.

L. Plaintiffs and the Class members suffered damages

146. The ramifications of Defendant's failure to keep employees' and former

employees' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.[32]

147. The PII belonging to Plaintiffs and Class members is private, sensitive in nature, and was left inadequately protected by Defendant who did not obtain Plaintiffs' or Class members' consent to disclose such PII to any other person as required by applicable law and industry standards.

148. Defendant required Plaintiffs and Class members to provide their PII, including full names and Social Security numbers in order to receive employment from Defendant. Defendant similarly required that Plaintiffs and Class members allow it to maintain that PII for the length of the employment relationship to receive elective benefits. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiffs and Class members in its possession was only used to provide agreed-upon employment and elective benefits from Defendant and that Defendant would not continue to maintain that PII once the employment relationship was terminated.

149. Plaintiffs and Class members therefore did not receive the benefit of the bargain with Defendant, because providing their PII to Defendant was in exchange for Defendant's implied agreement to secure it and keep it safe and to delete it following the end of the employment relationship. Had Plaintiffs and Class members known that Defendant would not safeguard their PII or would retain it well after they left the company, Plaintiffs and Class members would not have provided their PII, would have demanded higher pay, or would not have worked for Defendant at all.

---

[32] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed July 28, 2021).

150. Plaintiffs also were injured in that the Value of their PII has diminished as a result of the Data Breach. PII is a valuable property right and there is an active marketplace for non-public consumer date both on the dark web[33] and for legitimate enterprises who act as data brokers like Experian or Equifax. In 2019, the data brokering industry was worth roughly $200 billion.[34] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[3536] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[37] Nielsen also pay for consumers attention by paying them to monitor what programs they watch and for how long.[38] Accordingly, Plaintiffs and Class members have lost the ability to control how and where their PII is used and by whom.

151. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiff's and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII; (c) delete and destroy PII that it was not required to maintain; and (d) protect against reasonably foreseeable threats to the security or integrity of such information.

152. Defendant had the resources necessary to prevent the Data Breach, but

[33] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/
[34] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[35] https://datacoup.com/
[36] https://digi.me/what-is-digime/
[37] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed Mar. 29, 2021).
[38] https://markets.nielsen.com/us/en/about-us/panels/ratings-and-families/

neglected to implement adequate data security measures, despite its obligations to protect employees' PII.

153. Had Defendant remedied the deficiencies in its data security training and protocols and adopted security measures recommended by experts in the field, it would have prevented the intrusion leading to the theft of PII.

154. Had Defendant deleted or destroyed the PII of employees and former employees that it was not required to maintain, Plaintiffs and Class members would not have suffered the injuries described herein resulting from the Data Breach.

155. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

156. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[39]

157. As a direct result of the Defendant's failures to prevent the Data Breach, Plaintiffs and Class members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PII;

[39] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed July 28, 2021).

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

d. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII in its possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members.

158. In addition to a remedy for the economic harm, Plaintiff and Class members maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

159. To date, other than providing a woefully inadequate twelve (12) months of credit monitoring and identity protection services, Defendant does not appear to be taking any measures to assist Plaintiffs and Class members other than simply telling them to review their financial records and credit reports on a regular basis.

160. This type of recommendation, however, does not require Defendant to expend any effort to protect Plaintiffs' and Class members' PII.

161. Defendant's failure to adequately protect Plaintiffs' and Class members' PII has resulted in Plaintiffs and Class members having to undertake tasks requiring extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money – while Defendant sits by and does nothing to assist those affected by the Data Breach. Instead, as Defendant's notice letter indicates, it is putting the burden on Plaintiffs and Class members to discover possible fraudulent activity and identity theft and unfortunately Plaintiffs Vega and Granado have already experienced fraudulent activity as a result of the Data Breach.

162. Defendant's offer of twelve (12) months of identity monitoring and identity protection services to Plaintiffs and Class members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is acquired and when it is used. Furthermore, identity theft monitoring services only alert someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's PII) – they do not prevent identity theft.[40] Although their PII was improperly exposed in or about October 2021, affected current and former employees were not notified of the Data Breach until more than five months later, depriving them of the ability to promptly mitigate or even discover adverse consequences resulting from the Data Breach. As a result of Defendant's delay in detecting and notifying employees of the Data Breach, the risk of, and actual, fraud for Plaintiffs and Class members has been driven even higher.

[40] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited July 28, 2021).

CLASS ACTION ALLEGATIONS

163. Plaintiffs bring this action individually and on behalf of all members of the following class of similarly situated persons (collectively, the "Class" or "Class members"):

Nationwide Class

> All persons residing in the United States who are current or former employees, or job applicants, of SandRidge and had their PII compromised by an unknown third-party cybercriminal as a result of the Data Breach that occurred on or around October 25, 2021.

Excluded from the proposed Class are any officer or director of Defendant; anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

164. **Numerosity.** Members of the proposed Class likely number approximately twelve thousand and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendant's own records.

165. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class members and predominate over questions affecting only individual Class members. These common questions include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant's inadequate data security measures were a cause of the Data Breach;

c. Whether Defendant owed a legal duty to Plaintiff and the other Class members to exercise due care in collecting, storing, and safeguarding their PII;

d. Whether Defendant negligently or recklessly breached legal

duties owed to Plaintiff and the Class members to exercise due care in collecting, storing, and safeguarding their PII;

e. Whether Plaintiff and the Class are at an increased risk for identity theft because of the Data Breach;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices for Plaintiff's and Class members' PII in violation Section 5 of the FTC Act;

g. Whether Defendant improperly retained the PII of Plaintiffs and Class Members after the employment relationship ended or after it was no longer required to maintain the PII;

h. Whether Plaintiff and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

i. Whether Plaintiff and the other Class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

142. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

143. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the Class. All Class members were subject to the Data Breach and had their PII accessed by and/or

disclosed to unauthorized third parties. Defendant's misconduct impacted all Class members in the same manner.

144. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class members they seek to represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

145. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION
Negligence
(On behalf of Plaintiffs and the Nationwide Class)

146. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

147. As a condition of their employment or receiving elective benefits, Plaintiffs and Class members were obligated to provide Defendant with their PII.

148. Upon accepting and storing the PII of Plaintiffs and Class members on its computer systems and networks, Defendant undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class members could and would suffer if the PII was wrongfully disclosed. Plaintiffs and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class members had no ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiffs and the Class.

149. Because of this special relationship, Defendant required Plaintiffs and Class members to provide their PII, including names, Social Security numbers, and other personal information.

150. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiffs and Class members in its possession was only used to provide the agreed-upon compensation and other employment benefits from Defendant and that Defendant would destroy any PII that it was not required to maintain.

151. As part of this special relationship, Defendant had a duty to perform with skill, care, and reasonable expedience and faithfulness with regard to providing the agreed-upon compensation and other employment benefits to Plaintiffs and Class members and protecting Plaintiffs' and Class members' PII.

152. Through Defendant's acts and omissions, including Defendant's failure to

provide adequate security, its failure to protect Plaintiffs' and Class members' PII from being foreseeably accessed, and its improper retention of PII it was not required to maintain, Defendant negligently failed to observe and perform its duty.

153. Plaintiffs and Class members did not receive the benefit of the bargain with Defendant, because providing their PII was in exchange for Defendant's implied agreement to secure and keep it safe and to delete it once no longer required.

154. Defendant was aware of the fact that cyber criminals routinely target large corporations through cyberattacks in an attempt to steal customer and employee PII.

155. Defendant owed Plaintiffs and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard or delete such data and providing notification to Plaintiffs and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

156. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

157. Defendant had duties to protect and safeguard the PII of Plaintiffs and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive PII. Additional duties that Defendant owed Plaintiffs and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class members' PII was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiffs' and Class members' PII in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its networks and servers; and

d. To promptly notify Plaintiffs and Class members of any data breach, security incident, or intrusion that affected or may have affected their PII.

158. Plaintiffs and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and Defendant. Defendant was in a position to ensure that its systems were sufficient to protect the PII that Plaintiffs and the Class had entrusted to it.

159. Plaintiffs' injuries and damages, as described herein, are a reasonably certain consequence of Defendant's negligence and breach of its duties.

160. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class members' PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, and protecting the PII in its possession;

b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to consistently enforce security policies aimed at protecting Plaintiffs and the Class's PII;

d. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

e. Failing to promptly notify Plaintiffs and Class members of the Data Breach that affected their PII.

161. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

162. As a direct and proximate result of Defendant's negligent conduct, including but not limited to its failure to implement and maintain reasonable security practices and procedures as described above, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

163. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the PII of Plaintiffs and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class members while it was within Defendant's possession and control.

164. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class members, Defendant prevented Plaintiffs and Class members from taking meaningful, proactive steps to securing their PII and mitigating damages.

165. Plaintiffs and Class members could have taken actions earlier had they been timely notified of the Data Breach.

166. Plaintiffs and Class members could have enrolled in credit monitoring, could have instituted credit freezes, and could have changed their passwords, among other things, had they been alerted to the Data Breach more quickly.

167. Plaintiffs and Class members have suffered harm from the delay in notifying them of the Data Breach.

168. As a direct and proximate cause of Defendant's conduct, including but not limited to its failure to implement and maintain reasonable security practices and procedures, Plaintiffs and Class members have suffered, as Plaintiffs have, and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the publication and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii)

the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives. Thus, Plaintiffs and the Class are entitled to damages in an amount to be proven at trial.

169. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's negligent conduct.

170. Plaintiffs and the Class have suffered injury and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On behalf of Plaintiffs and the Nationwide Class)

171. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

172. Defendant offered employment, compensation, and other elective benefits to Plaintiffs and Class members in exchange for their PII and labor.

173. Defendant required Plaintiffs and Class members to provide their PII, including names and Social Security numbers, and other personal information. In exchange Defendant promised to keep the PII of Plaintiffs and Class members safe from unauthorized access and to delete or destroy the PII once the employment relationship ended or it was no longer necessary to maintain the PII.

174. Plaintiffs and Class members, had they known that Defendant would not keep their PII secure or that Defendant would continue to possess it for years after their employment ended, would have demanded higher pay or chosen to take other employment and not be

employed by Defendant.

175. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiffs and Class members in its possession was only used to provide the agreed-upon compensation and other elective employment benefits from Defendant.

176. These exchanges constituted an agreement between the Parties: Plaintiffs and Class members would provide their PII for a limited period of time in exchange for employment and benefits provided by Defendant. No reasonable person would have provided their PII to Defendant without a promise to safeguard it and no reasonable person would have provided their PII to Defendant to retain for its own uses for years after the employment ended.

177. These agreements were made with Plaintiffs as an inducement to being employed by Defendant.

178. It is clear from these exchanges that the parties intended to enter into an agreement. Plaintiffs and Class members would not have disclosed their PII to Defendant but for Defendant's promise of compensation and other employment benefits and Defendant promise to safeguard and delete their PII. Defendant presumably would not have taken Plaintiffs' and Class members' PII if it did not intend to provide Plaintiffs and Class members compensation and other employment benefits. Nor could Defendant reasonably infer from the circumstances of the transaction that safeguarding the PII was a not necessary obligation or that it could maintain the PII for purposes unrelated to employment, i.e., after the relationship ended.

179. Defendant was therefore required to reasonably safeguard and protect the PII of Plaintiffs and Class members from unauthorized disclosure and/or use and to delete it following the end of the employment relationship.

180. Plaintiffs and Class members accepted Defendant's employment offer and fully performed their obligations under the implied contract with Defendant by providing their PII, directly or indirectly, to Defendant, among other obligations.

181. Plaintiffs and Class members would not have provided and entrusted their PII to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PII for uses other than compensation and other employment benefits from Defendant.

182. Plaintiffs and Class members did not provide their PII for non-employment purposes and Defendant had no reason to retain it following the end of the employment term

183. Defendant breached the implied contracts with Plaintiffs and Class members by failing to reasonably safeguard and protect Plaintiffs' and Class members' PII.

184. Defendant's failure to implement adequate measures to protect the PII of Plaintiff and Class members violated the purpose of the agreement between the parties: Plaintiffs' and Class members' employment in exchange for compensation and benefits.

185. Defendant was on notice that its systems could be vulnerable to unauthorized access yet failed to invest in proper safeguarding of Plaintiffs' and Class members' PII.

186. Instead of spending adequate financial resources to safeguard Plaintiffs' and Class members' PII, which Plaintiffs and Class members were required to provide to Defendant, Defendant instead used that money for other purposes, thereby breaching its implied contracts it had with Plaintiff and Class members.

187. While Defendant had discretion in the specifics of how it met the applicable laws and industry and contractual standards, this discretion was governed by an implied covenant of good faith and fair dealing.

188. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations when it engaged in unlawful practices under other laws. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiffs' and Class members' PII; storing the PII of former employees despite any valid purpose for the storage thereof ceasing upon terminating the relationship with those individuals; and failing to disclose to Plaintiffs and Class members at the time they provided their PII to it that Defendant's data security systems, including training, auditing, and testing of employees, improperly retained the PII of Plaintiffs and Class members after it was no longer necessary, and failed to meet applicable legal and industry standards.

189. Plaintiffs and Class members did all or substantially all the significant things that the contract required them to do.

190. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiff and Class members, Plaintiffs and the Class members suffered injury as described in detail in this complaint and are entitled to damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On behalf of Plaintiffs and the Nationwide Class)

191. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

192. Plaintiffs bring this claim in the alternative to the breach of contract claim above.

193. Plaintiffs and the Class Members conferred a monetary benefit on Defendant by providing their PII which Defendant required as a condition of their employment. Plaintiffs and Class members provided their PII and accepted employment on the condition that

Defendant safeguard their PII and delete it once it was no longer required to retain it.

194. Plaintiffs and Class Members conferred a monetary benefit on Defendant in that Defendant derived revenue from their labor, a precondition of which required Plaintiffs and Class members to entrust their PII to Defendant. Without the labor and PII provided by Plaintiffs and Class members, Defendant could not derive revenue from its regular business activities. A portion of the revenue derived from the labor and PII of Plaintiffs and Class members was to be used to provide a reasonable level of data security and practices, and the amount of revenue to be allocated to data security is known to Defendant.

195. Defendant knew that Plaintiffs and Class Members conferred a benefit on it and Defendant accepted that benefit. Defendant derived revenue from the labor and PII of Plaintiffs and the Class and rather than use a portion of that revenue to protect the PII of Plaintiffs and the Class it instead diverted that money to its own profit.

196. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class members' PII. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

197. Under the principles of equity and good conscience, Defendant should not be permitted to retain the profits it wrongfully derived from Plaintiffs and Class members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

198. Defendant failed to secure Plaintiffs' and Class members' PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class members provided. Defendant has money in its hands that in equity and good conscience, it should not be permitted to retain.

199. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged and that it diverted money intended to protect Plaintiffs and the Class to its own profits.

200. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their PII, they would not have agreed to provide their PII or labor to Defendant.

201. Plaintiffs and Class Members have no adequate remedy at law.

202. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their PII is used; (c) the compromise, publication, and/or theft of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and

Class members.

203. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm.

204. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that they unjustly received from them.

FOURTH CAUSE OF ACTION
Declaratory and Injunctive Relief
(On behalf of Plaintiffs and the Nationwide Class)

205. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

206. As previously alleged and pleaded, Defendant owes duties of care to Plaintiffs and Class members that require it to adequately secure their PII.

207. Defendant still possesses the PII of Plaintiffs and the Class members even after their employment relationship ended and Defendant was no longer required to maintain it.

208. Defendant has not satisfied its obligations and legal duties to Plaintiffs and the Class members.

209. According to the Notice Letter, Defendant is taking some steps to increase its data security but it is unclear whether those steps are adequate or whether Defendant intends to retain ex-employee PII. Moreover, there is nothing to prevent Defendant from reversing these changes once it has weathered the increased public attention resulting from this Data Breach, and to once again place profits above protection.

210. Plaintiffs, therefore, seek a declaration that (1) Defendant’s existing security measures do not comply with its contractual obligations and duties of care to provide adequate

security, and (2) to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering Defendant to engage third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering Defendant to significantly increase its spending on cybersecurity, including systems and personnel;

c. Ordering Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;

d. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner any PII not necessary for its provisions of services;

f. Ordering that Defendant conduct regular database scanning and securing checks;

g. Ordering Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

h. Ordering Defendant to implement and enforce adequate retention policies for PII, including destroying PII as soon as it is no longer necessary for it to be retained;

i. Ordering Defendant to meaningfully educate its employees about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves; and

j. Ordering that Defendant remove former employees' PII from any hard drive or server that has external (Internet) access.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, respectfully request that the Court enter an order:

a. Certifying the proposed Class as requested herein;

b. Appointing Plaintiffs as Class Representative and the undersigned counsel as Class Counsel;

c. Finding that Defendant engaged in the unlawful conduct as alleged herein;

d. Granting injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the PII of Plaintiffs and Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class members;

iv. requiring Defendant to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the PII of Plaintiffs' and Class members' PII;

v. prohibiting Defendant from maintaining Plaintiffs' and Class members' PII on a cloud-based database;

vi. requiring Defendant to engage independent third-party

security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with

handling PII, as well as protecting the PII of Plaintiffs and Class members;

xii. requiring Defendant to conduct internal training and education routinely and continually and, on an annual basis, inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect

themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers;

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

xviii. requiring Defendant to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected;

xix. requiring Defendant to detect and disclose any future data breaches in a timely and accurate manner;

xx. requiring Defendant to implement multi-factor authentication requirements, if not already implemented;

xxi. requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; and

xxii. requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class

members.

e. Awarding Plaintiffs and Class members damages;

f. Awarding Plaintiffs and Class members pre-judgment and post-judgment interest on all amounts awarded;

g. Awarding Plaintiffs and the Class members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Class, hereby demand a trial by jury as to all matters so triable.

Date: September 2, 2022

Respectfully Submitted,

/s/ William B. Federman
William B. Federman, OBA #2853
FEDERMAN & SHERWOOD
10205 N. Pennsylvania
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com
*Pro hac vice forthcoming

Attorneys for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that all counsel of record who are deemed to have consented to electronic service are being served on September 2, 2022 with a copy of this document via the Court's CM/ECF system per Local Rule CV-5. Any other counsel of record or unrepresented party will be served by electronic mail, facsimile transmission and/or first class mail on this same date.

/s/ William B. Federman
William B. Federman